Growing Cybersecurity Risks in the Municipal Bond Market

Jul 30, 2025

Categories:

Matters of Interest
Publications

Authors:

Ben Hadden
Chris Ansell

In November 2024, the Township of White Lake, Michigan, fell victim to a cyberattack resulting in the wiring of approximately $29 million to the unauthorized account of the culprit. Before White Lake imminently closed on its issuance of general obligation bonds to finance new governmental buildings, the hacker was able to access the township's email system, impersonating an official of the township and sending altered wiring instructions to the underwriter of the bond. At the closing, instead of the township account, the purchase price was wired to the hacker. The sale of the bonds was ultimately canceled, and to this date, only approximately $21 million of the purchase price has been recovered. The underwriter is suing the township for the remainder.

Cyberattack Frequency and Disclosures

In recent years, there has been an increase in the frequency and media coverage of cyberattacks, from phishing scams to ransomware, and corporations are constantly working to stay ahead of bad actors by improving policy and technology. As evidenced by the White Lake cyberattack, the municipal markets are not immune to this threat—in fact, the public sector was the third most targeted sector by foreign nation-state cyber threat actors in 2024, according to Microsoft Threat Intelligence's global 2024 Digital Defense Report.

Tracking the rate of these incidents in the municipal market can be difficult, as there are currently no official guidelines from the Securities and Exchange Commission (SEC) pertaining to municipalities and their disclosure of cybersecurity risks or attacks. Issuers may be hesitant to make such disclosures for fear of the negative impact on their credit ratings and the associated negative publicity. This hesitation is well founded: two issuers, one in California and one in Maryland, recently had their credit downgraded after suffering cyberattacks. However, experts believe that, despite the potential credit impact, disclosure is essential, as it

allows law enforcement to better understand cyberattack trends, build their databases, and develop strategies to prevent future attacks.

Additionally, despite the SEC having no direct regulatory authority over municipal issuers, it is nevertheless investigating the Township of White Lake for possible securities law violations in connection with the 2024 cyberattack. The SEC is reviewing the incident through the lens of federal antifraud provisions that apply to all capital markets participants, mainly that investors are entitled to be informed of all "material" information related to securities. Here, the SEC may investigate whether White Lake accurately described the incident to investors and whether the township is fully disclosing its ongoing vulnerabilities, remediation costs, and possible impacts on its finances. All of these items would likely be deemed material, thus requiring proper disclosure by White Lake to avoid running afoul of antifraud provisions.

Cyberattack Prevention in the Municipal Market

For most governmental units, bond financings are non-routine occurrences. A bond transaction is complex, involving multiple parties such as underwriters, financial advisors, and paying agents with whom the staff of the issuer may be unfamiliar. This unfamiliarity and complexity, combined with heavy reliance on electronic communication, create an environment ripe for bad actors to take advantage of the parties involved.

Cybercriminals have capitalized on human error as much as technological weakness, and local government is arguably the least mature sector in terms of cybersecurity. In response, the Government Finance Officers Association (GFOA) has compiled a list of key fraud prevention measures that issuers should apply when receiving or sending funds. GFOA's recommendations are as follows:

- Communication to other parties that no change of banking information will be sent via email, and any emails indicating such changes should be considered fraudulent;

- Communicate to other parties that the issuer will notify them only by telephone or video meeting of any changes to the issuer's banking information, and ask for other parties to verify that they understand this policy;
- Banking and financial information sent to the deal team should be encrypted;
- Communicate to other parties that if an email is received, they should utilize their own contact information to contact the issuer, and not the information listed in the email;
- For bond proceeds, all parties involved in the transfer of funds should have a video call confirming the wire instructions, including the trustee if applicable;
- When possible, use good faith deposits or test payment information with a small payment amount before having the full amount of funds sent; and
- The issuer should have the bank/payor utilize payee confirmation systems before sending funds.

Additionally, in response to the growing cybersecurity issue, third-party providers have begun offering services to secure certain municipal transactions, including multifactor identification, identity verification, and micro-depositing.

Is Cyber Insurance Sufficient Protection?

Bond issuers have also been obtaining cyber insurance as a means to protect themselves and potential investors from cybercrimes. However, industry experts are clear in their sentiment that while cyber insurance is important, it does not solve the root problem; insurance is *not* a substitute for security and policy. Cyber insurance is also expensive, with premiums projected to rise by 15% to 20% annually by the end of 2026. Additionally, insurance providers have become more creative with insulating themselves from risk, and the denial of coverage rates are high.

In recent years, audits of the insured's systems have become more frequent and stricter, resulting in denials of coverage for the insured if they are not performing to at least industry standards. Further,

large providers have begun to deny coverage if the attack can be connected to a nation-state actor. There has been a notable increase in cyberattacks conducted by nation-state actors targeting state and local governments in the last two years, partially due to adversarial nation-states not differentiating between local governments and the federal government. They view it as just an attack on the United States. Additionally, due to the United States' transparency laws, these hostile actors have easier access to smaller units of government that may be less sophisticated or cognizant of threats.

Key Takeaways for Local Government Going Forward

Traditionally, the municipal market looks to the more regulated corporate market and mirrors its policies. The SEC has provided very specific rules for the corporate securities market around disclosure relating to cyberattacks, and many participants in the municipal market are calling for implementation of similar rules. For example, in 2023, the SEC implemented a rule standardizing cybersecurity disclosure for public companies, requiring that they report material cybersecurity incidents within four days.

The SEC has indicated that many principals applicable to the registered market can be applied to the municipal market, and some municipal issuers have begun to take actions that align with the SEC rules for the registered market. For instance, some municipal issuers have begun including their cybersecurity insurance in offering documents to inform potential investors that they are aware of the cybersecurity risk and are taking steps to mitigate it.

Ultimately, as the frequency and cost of these attacks continue to increase, disclosure of cybersecurity-related information in the offering documents of municipal issuers will become more common and more important than ever. Pending any regulation, municipal issuers and market participants will need to cooperate to standardize best practices. Such discussions are already in process and taking place at industry forums and within professional associations.

For questions or assistance as it relates to cybersecurity and the municipal market, please contact the authors or any attorney with Frost Brown Todd's Public Finance Practice Group.

FBT Gibbons